Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: **2/22/2010**

Name of company covered by this certification: **Cosmobridge America, Inc.**

Form 499 Filer ID: **827434**

Name of signatory: **Doo Sik Shin**

Title of signatory: **C.E.O.**

I, **Doo Sik Shin**, certify that I am an officer of **Cosmobridge America, Inc.** (the company named above, herein referred to as "the company"), and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*, which is a subpart to implement **section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222**.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. See attached accompanying statement for details.

The company has not had to taken any actions in the form of proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers in the past year.

The company understand that it must report on any information that it has with respect to the processes pretexters are using to attempt to access CPNI , and what steps the company is taking to protect CPNI.

Note, the company recognizes "pretexting" as "the process in which personal information is obtained by fraudulent means including identity theft, selling personal data for profit, or using some other method for snooping for information whose release was not authorized by the owners of the information. See attached accompanying statement for details on how the applicant guards CPNI data against pretexting.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI and the company has received **0 number of customer complaints** received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint as follows:

(1) Instances of improper access by employees: **0 complaints**
(2) Instances of improper disclosure to individuals not authorized to receive the information: **0 complaints**
(3) Instances of improper access to online information by individuals not authorized to view the information: **0 complaints**

If it was affirmative, the company would have provided summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R.§ 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attached Accompanying Statement

The followings are **the measures put in place by the carrier** (herein referred to as "the company") to protect CPNI from pretexting. The company understands that the three common types of "pretexting" are identity theft, selling personal data for profit without authorization by the owner or using some other method for snooping for information whose release was not authorized by the owner of the information.

I. pretexting via identity theft
   (A) Identity theft via theft of physical hardware containing CPNI data
   Guarding Measures:
   The company utilizes physical security such as locks and security surveillance to protect physical hardware and limits physical access to authorized personnel. Also certain portable hardware such as laptops have security features that provide additional security.

   (B) Identity theft via hacking/virtual intrusion of systems that carry CPNI
   Guarding Measures:
   The company utilizes security software to detect and prevent unauthorized access via hacking and other virtual methods.

II. Pretexting via some other method for snooping for information whose release was not authorized by the owner
   (A) Snooping via social engineering/impersonation/false identification
   Guarding Measures:
   As a calling card provider, the company doesn't acquire any detailed customer information. Only information the company has is the phone number customer use.

   (B) Snooping by personnel not authorized to access data
   Guarding Measures:
   The company limits access of CPNI to authorized personnel only.

III. Pretexting by selling CPNI for profit without authorization by the owner
   (A) Selling CPNI data by the company with other companies
   Guarding Measures:
   The company does not share CPNI data with other companies for marketing and profit purpose.